中国科学院审计信息系统管理规范（试行）

第一章 总则

第一条 为规范中国科学院审计信息系统（Audit Information System，以下简称AIS系统）的操作流程，提高信息化审计的工作效率，保证审计数据的安全，明确在AIS系统运行和维护中的职责、权利和义务特制定本规范。

第二条 院内部审计机构或人员利用AIS系统开展审计工作、实施审计作业时应遵循本规范。

第三条 本规范的主要内容：

系统的运行管理是指审计人员利用AIS系统开展审计的工作要求。

系统的维护是指为确保AIS系统正常、稳定运行对AIS系统硬件、软件及数据库的管理。

信息安全是指为确保使用AIS系统过程中数据安全，防止泄漏、丢失和损坏数据所制定的数据的使用范围与规则。

第二章 系统运行管理

第四条 院各级内部审计机构应配备至少1名有信息化管理工作经验的人员作为AIS系统管理员，负责本机构AIS系统的日常管理工作。

第五条 各分院内审机构应依据本规定相关授权，结合自身管理情况，制定本分院系统的AIS系统运行管理办法。

第六条 在AIS系统上线运行后，实施审计工作管理，开展计划内审计工作应使用本AIS系统。

第七条 AIS系统运行流程：

（一）计划管理：监察审计局（以下简称监审局）对审计项目实施计划管理，制定全院年度审计工作计划并上传至AIS系统。各分院内部审计机构根据需求和工作安排制定本分院系统年度审计工作计划并上传AIS系统。

具备条件的所级内审机构根据需求和工作安排制定本单位年度审计工作计划并纳入分院年度审计工作计划一并上传AIS系统。

（二）数据采集与转换：原则上由监审局将被审计单位的ARP数据转换为AIS系统可读的审计数据；监审局亦可授权具备条件的分院内审机构开展数据的采集与转换工作。具有数据采集转换权限的内审机构要根据年度工作计划提前采集转换各被审计单位的ARP数据。

（三）启动项目：监审局、分院内部审计机构应根据审计工作计划启动审计项目，组成审计工作组，并根据审计调查的情况上传项目审计方案、审计通知。

（四）数据分析：审计项目主审应对转换数据的准确性、完整性、系统性进行复核，测试ARP信息环境下内部控制关键环节的执行情况；采取恰当的方法（结构、趋势、比例分析）了解被审单位经济活动规律，筛选审计线索，确定审计的范围和重点。

（五）编制底稿：审计组成员在审计工作期间应在线填写审计底稿，并将审计证据作为底稿附件上传。通过AIS系统收集的以电子资料、计算机存储或处理形式获取的审计证据，必要的情况下可打印成纸质材料由被审计单位和个人盖章或签名。

审计人员应当对审计的过程做必要的记录，按时编制和上传审计工作日记，以保证可重现审计过程。

（六）复核工作底稿：审计工作终结前由项目主审对审计过程中上传的过程文档及审计工作底稿、审计证据进行复核，确定AIS系统记录的完整性、准确性。

（七）终结项目：审计工作结束后，项目主审应将审计报告及时上传AIS系统，按照审计档案归档要求整理出电子档案，确认审计电子档案的完整性后，及时终结审计项目。

（八）数据的清理：监审局、分院内审机构信息管理员应定期（一般为项目终结6个月后）对已终结审计项目采集的数据予以清除。

第八条 院各级内部审计机构应及时对审计工作进行数据汇总与统计，总结审计案例与管理案例。

第三章 系统的维护管理

第九条 监审局负责AIS系统运行维护和管理总体工作。

第十条 监审局审计监察室具体负责硬件设备维护，协调院网络中心提供服务器日常运行的工作环境和网络环境，完成VPN系统用户添加及权限分配。

第十一条 软件维护工作委托软件开发方承担。监审局负责监控系统软件维护的效果，并对维护服务的质量进行评估。

第十二条 监审局负责管理AIS系统数据的授权，监审局与分院内审机构AIS系统管理员根据授权对AIS系统数据库进行维护和管理。

监审局AIS系统管理员对AIS系统的被审计单位库、法律法规库、机构信息库开展日常管理和定期的更新工作，根据分院的申请及时更新分院AIS系统用户信息。

各分院内部审计机构负责管理本级AIS系统的中介机构库、审计人才库、审计方案库、审计经验库、审计案例库。根据内部审计人员岗位变化的情况及时向监审局提交《审计信息系统注销用户申请表》和《审计信息系统增加用户申请表》对系统用户进行及时的更新。

第四章 信息安全管理

第十三条 AIS系统设有权限管理体系，权限体系未经监审局同意，各分院AIS系统管理员不得进行修改。

第十四条 监审局与分院内审机构AIS系统管理员是AIS系统安全的具体责任人，负责所辖AIS系统的信息安全工作，定期对AIS系统的人员权限、信息资源进行检查，查找各类信息安全隐患，保证AIS系统安全运行。

第十五条 具有数据采集权限的各级AIS系统管理员负责对审计电子数据的采集、转换和清除进行管理，并承担数据保密责任。监审局负责管理被审计单位的审计VPN和数据库的接入方式，并承担保密责任。

第十六条 院、分院内审机构自行增加临时项目，应填写《审计信息系统采集ARP数据申请表》并上报监审局，经监审局审核同意后根据项目实施的情况和权限对该项目数据进行管理（立项、延期、注销、数据清理），确保数据安全。

第十七条 按照审计项目负责制的原则，采集完成的原始审计电子数据文件，由审计项目现场负责人进行保管和监控。不得将原始审计电子数据拷贝给除监审局AIS系统管理员之外的其他人。

第十八条 在审计项目开始前审计组成员应签订《审计信息系统操作保密责任书》。对使用AIS系统实施审计过程中取得的“审计电子数据”使用的安全承担责任，防止无关人员接触和复制审计电子数据。不得私自保留审计电子数据。

第五章 附则

第十九条 院监审局负责对各分院内部审计机构使用AIS系统审计的绩效进行定期考核。

第二十条 委托中介机构实施的审计项目暂不使用AIS系统，各单位不得为非院内部审计人员开通临时账户

第二十一条 审计人员在使用AIS系统实行审计的过程中存在以下情况之一的，应对直接责任人追究管理责任。

1、导致ARP系统安全责任事故或涉密信息泄密，被有关部门追究责任的。

2、在使用AIS系统审计过程中，由于疏忽或严重操作失误，造成AIS系统运行出现故障或瘫痪的，或因管理不严造成电子数据泄密的。

3、计划内审计项目因主观原因未上线实施的。

第二十二条 本规则由监审局负责解释。本规则自下发之日起施行。

|  |
| --- |
| **审计信息系统采集ARP数据申请表** |
| 单位： |  |  |  |
| 申请人 |  | 内审机构 |  |
| 申请日期 |  | 审计实施日期 |  |
| 临时项目名称 |  |
| 被审计单位 |  | 审计期间 |  |
| 需采集数据期间 |  |
| 项目关闭日期 |  |
| 机构领导审批 |  |
| 主管领导审批 |  |
|  |  |  |  |
| 注：项目关闭日期即为采集的ARP数据清理日期。 |  |

|  |
| --- |
| **审计信息系统增加用户申请表** |
| 申请人 |  | 出生年月 |  | 性别 |  |
| 单位 |  | 隶属分院 |  |
| 部门 |  | 职称 |  | 职务 |  |
| 毕业院校 |  | 专业 |  |
| 学历 |  | 申请日期 |  |
| 部门领导审批 |  |
| 主管领导审批 |  |

|  |
| --- |
| **审计信息系统注销用户申请表** |
| 申请人 |  | 用户名 |  |
| 单位 |  | 隶属分院 |  |
| 申请日期 |  | 注销原因 |  |
| 部门领导审批 |  |
| 主管领导审批 |  |